財團法人台灣網路資訊中心因公出國人員報告書 108 年 8 月 2 日

報告人 姓　名	顧靜恆 許乃文 林福寬	服務單位及 職稱	組長 組長 工程師
出國期間	108/7/19-28	出國地點	Montreal, Canada
出國事由	參加 IETF 105 Montreal Meetings		

報告書內容包含：
一、 出國目的
二、 會議行程
三、 考察、訪問心得
四、 建議意見
五、 會議議程

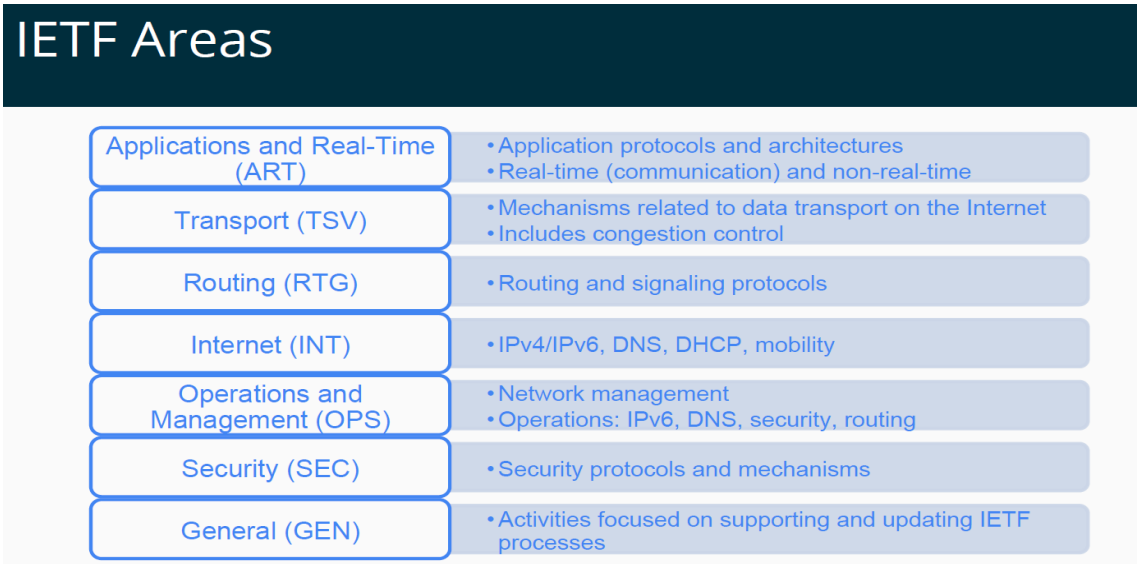
授　權 聲 明 欄	本出國報告書同意貴中心有權重製發行供相關研發目的之公開利用。 授權人： 顧靜恆 許乃文 林福寬 (簽章)

註
二、請於授權聲明欄簽章，授權本中心重製發行公開利用。
附一、請以「A4」大小紙張，橫式編排。出國人員有數人者，依會議類別或考察項目，彙整提出報告。

一、 出國目的：

參加 IETF 105 Montreal 會議。

這是 IETF（網際網路工程任務小組, Internet Engineering Task Force）所舉辦的第 105 次會議，於 2019 年 07 月 20 日（星期六）至 2019 年 07 月 26 日（星期五）在加拿大蒙特婁召開，總共為期七天的會議，是由 COMCAST 與 NBCUniversal 共同主辦。本次參與會議人數高達 1,961 人，其中有 859 人是利用遠端會議系統的方式參與。會議主題共分為以下 7 大項目：



中心參加此次會議的主要目的為參與及了解各 WGs（Working Groups，工作小組）技術發展的趨勢及討論方向，包含 DNS、Security、EPP、IPv6 及 IoT 等相關議題。

Working Groups 是制定 IETF 技術規格和規範的主要機制，各小組負責不同技術規格的討論，並接收各方的意見加以修改，最終目的是要讓技術規格成為網際網路運作的標準或建議書，提供網際網路的技術開發團隊能有技術標準規格可做為依循，及保障全球網際網

路能通行無礙。WGs 的運作方式是透過建立一個新的章程，該章程定義特定問題及成果(包含建議、標準規範等)。各 Working Group 會有一位主席追蹤小組的運作狀況，並在章程規定小組的工作範圍，列出如何完成此項工作的目標和里程碑等資訊，每個 Working Group 都是由和其本身工作領域相關的技術人員參與。當完成目標後，Working Group 就會結束，但有些 Working Group 會隨著環境及應用的變化，不斷改進已建立的標準協議，則此 Working Group 就會持續維持運作狀態。所有進行中的 Working Group 可以在 IETF Datatracker 找到完整列表。

IETF Datatracker 查詢網站：https://datatracker.ietf.org/

圖：IETF 105 大會報到處

二、 會議行程：

詳如會議網站 https://www.ietf.org/how/meetings/105/ 。
議程 https://datatracker.ietf.org/meeting/105/agenda.html 。
IETF 網站 https://www.ietf.org/ 。

參與會議的行程安排如下表列：

日期	時間	議程
108/7/20 (六)	8:30-22:00	IETF Hackathon
108/7/21 (日)	8:30-16:00	IETF Hackathon
	10:00	IETF Registration
	12:30-13:30	Tutorial: Newcomers' Overview
	16:00-17:00	Newcomers' Quick Connections
108/7/22 (一)	8:00-9:00	Continental Breakfast
	9:00-19:10	IRTF Applied Networking Research Workshop (ANRW)
	10:00-12:00	Routing Area Working Group
	12:00-13:30	Break
	13:30-15:30	IPv6 over Networks of Resource-constrained Nodes WG
	15:30-15:50	Beverage and Snack Break
	15:50-17:50	IPv6 Operations WG
	18:10-19:10	Domain Name System Operations WG
108/7/23 (二)	8:00-9:00	Continental Breakfast
	10:00-12:00	Domain Name System Operations WG
	11:30-12:00	IP Wireless Access in Vehicular Environments WG
	12:00-13:30	Break
	13:30-15:00	Applications Doing DNS WG
	13:30-15:00	Security Events WG
	15:00-15:20	Beverage and Snack Break
	15:20-16:50	SIDR Operations WG
	17:10-18:10	IPv6 Maintenance

108/7/24 (三)	8:00-9:00	Continental Breakfast
	10:00-12:00	Software Updates for Internet of Things WG
	12:00-13:30	Break
	13:30-15:30	Thing-to-Thing WG
	15:30-15:50	Beverage Break
	15:50-16:50	Global Routing Operations WG
	16:50-17:10	Beverage and Snack Break
	17:10-18:10	IETF Technical Plenary
	18:20-19:50	IETF Administrative/Operations Plenary
108/7/25 (四)	8:00-9:00	Continental Breakfast
	10:00-12:00	Interface to Network Security Functions WG
	12:00-13:30	Break
	13:30-15:30	Extensions for Scalable DNS Service Discovery WG
	15:30-15:50	Beverage and Snack Break
	15:50-17:20	IPv6 Maintenance WG
	15:50-17:20	DNS PRIVate Exchange WG
	17:20-17:40	Beverage Break
	17:40-19:10	IPv6 over the TSCH mode of IEEE 802.15.4e WG
108/7/26 (五)	8:00-9:00	Continental Breakfast
	10:00-12:00	IPv6 over Low Power Wide-Area Networks WG
	12:00-12:20	Beverage and Snack Break
	12:20-13:50	Inter-Domain Routing WG

三、 考察、訪問心得：

IETF 105 Montreal 會議

圖：IETF 105 會場

於本次會議中，主要參與的主題包含 Hackathon、ANRW(Applied Networking Research Workshop)、DNS、註冊協議擴展(Registration Protocols Extensions)、IPv6 及 IoT 等領域的相關議題，分別整理如下：

Hackathon

Hackathon 活動是 IETF 為鼓勵開發人員能在一個開放且協作的環境中，依據不同的主題分組面對面討論、交換彼此的想法、演示程式代碼、及尋求解決方案。任何的競爭都是良性的，並且秉持著持續發展新的或改良現有互聯網標準的精神前進。

本次 Hackathon 活動參與人數約有 384 名，分成 30 個不同的主題分組討論，並於第二天下午由各組進行 3 分鐘的簡短報告(下載連結)。此次會議主要參與 DNS 主題，內容包含：

1. DNS privacy：Zone transfers over TLS、DoH proxy plugin for any webserver、Preparing BIND for DoT/DoH。

2. DNS support for specific network environments：Identifier/Locator Network Protocol RRs、DNS64 prefix discovery。
3. DNS provisioning：Interoperable DNS server cookies、Timeout RR、HTTPSSVC。

圖：Hackathon 活動分組討論現況

詳細的 Hackathon 說明及參與方式，可以參考以下網址：
https://trac.ietf.org/trac/ietf/meeting/wiki/105hackathon

ANRW(Applied Networking Research Workshop)

ANRW 2019 是一個學術研討會，為研究人員、供應商、網路營運商和網際網路標準社群提供一個展示和討論研究新成果的論壇，也提供了一個機會，讓研究學者們，可以將其研究轉為 IETF 標準或協議，並且可以從討論的過程及公開的問題中，獲得新的靈感。本次研討會是由 ACM SIGCOMM 公司及 IRTF(Internet Research Task Force)所贊助。

此次 ANRW 所報告的主題，包含以下的內容：

1. A Performance Perspective on Web Optimized Protocol Stacks: TCP+TLS+HTTP/2 vs. QUIC

比較現有瀏覽網頁的連線方式（TCP+TLS+HTTP/2）與未來預計使用的 QUIC 連線方式，兩者之間的性能差異。雖然傳統的連線方式，可以利用 TCP 參數的優化，讓 Web 堆疊的性能直接產生顯著的改進，但，QUIC 的性能仍高於優化後的 TCP。這種性能優勢主要是由於 QUIC 在連接建立期間減少了 RTT 設計，並且由於其能夠繞過線路阻塞而導致網絡損耗。

2. Performance Measurements of QUIC Communications

在數據封包遺失、延遲和抖動方面的性能量測，是現代網路封包交換的關鍵。這些數值也明確地呈現出網路供應商的服務品質(QoS)，特別是在用戶使用諸如語音、視訊會議之類的實時通信時影響最大。因此，針對 QUIC 提出了一種新的性能量測方法，並與該領域的現有方式進行比較，透過對測試環境的實驗驗證和評估來顯示這些結果。

3. Who Is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolution Path

用戶使用網路透過 DNS 服務來解析域名時，可以使用 ISP（Internet Service Providers）預設提供的 DNS 主機、也可以自由選擇喜歡的公共 DNS 主機（例如：168.95.1.1 或 8.8.8.8）。但，少數 ISP 公司可能會利用路由設定，將向公共 DNS 主機的查詢秘密攔截轉由自身的 DNS 主機回應，而產生隱私和安全的問題。因此，本文分析大量 DNS 攔截的特徵後，設計了新的檢測 DNS 攔截方法，並利用全球 148,478 個家用及行動網路的 IP 位址，在檢查的 3,047 個 ASec 中，發現有 259 個出現 DNS 攔截的行為。為了解決此類問題，提供了新的見解。

4. Oblivious DNS: Practical Privacy for DNS Queries

使用網際網路服務時，幾乎都需要使用到 DNS 查詢服務，因此，用戶所拜訪（查詢）過的網站（域名）、及用戶的 IP 位址皆因此而被 DNS 主機記錄，而存在隱私漏洞的隱憂。因此，本文提出了一個新的 Oblivious DNS(ODNS)概念，在用戶端與 DNS 主機之間加入一個模糊層，利用他當緩衝而隱藏用戶的 IP 位位，並且相容於現有的 DNS 架構。

5. Analyzing the Costs (and Benefits) of DNS, DoT, and DoH for the Modern Web

新型態的 DNS 查詢方式(Dot、DoH)，相較於傳統查詢方式(Do53)，雖然可以保護隱私，不會被窺視查詢的域名資料，但，卻必須額外付出成本（回應時間增加）。因此，本文比較這三種查詢方式，分析當網路流量正常、壅塞等狀況時，對於瀏覽網頁時的載入速度影響程度為何？實驗結果得知，在正常狀況時，DoT 的網頁載入速度優於 Doh 及 Do53；但當網路壅塞時，Do53 載入速度最快。文中也提到，可以採取 opportunistic partial responses 或 wire format caching 方式，就能輕鬆提升 DNS 性能。

6. What Can You Learn from an IP?

由於原始網際網路的設計並不符合安全性，為避免竊聽者取得（或推測）使用者瀏覽的網頁內容，因此發展出許多加密體系，例如：加密的 DNS、HTTPS 等。但，加密不一定能保證匿名性或隱私性，只需要觀察使用者設備流量上的目標 IP 位址，依然可以推測出訪問的網站（域名）。

詳細的 ANRW 介紹，可以參考以下網址：https://irtf.org/anrw/2019/

DNS 相關技術討論

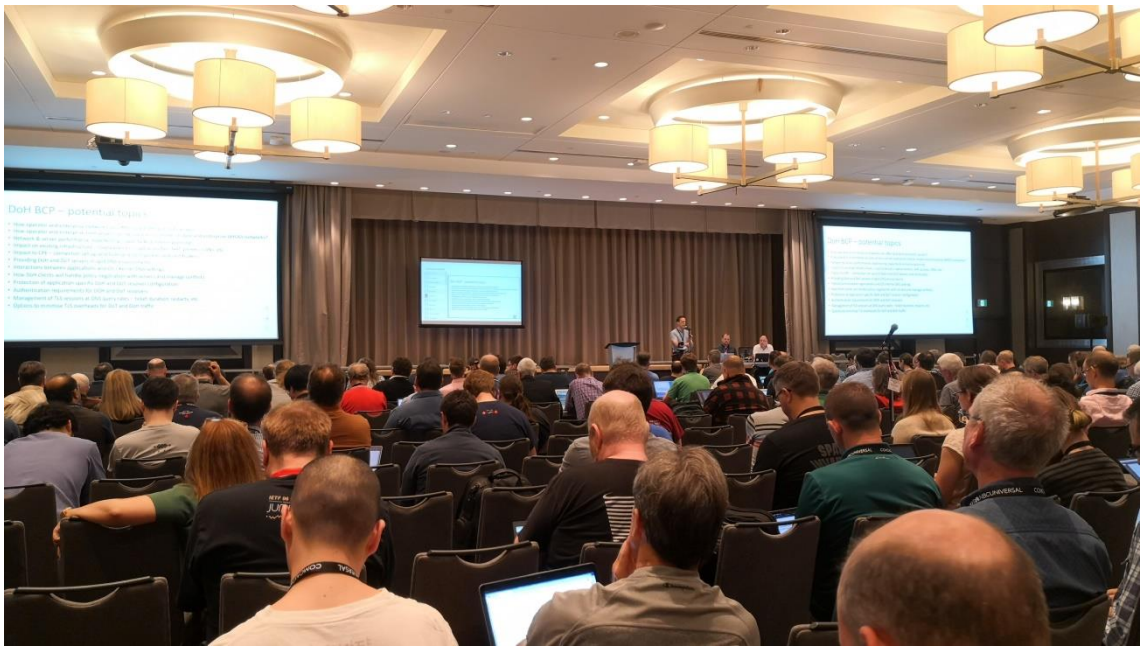
DNS 在工作小組的報告項目中，有幾個新式資源記錄雖然目前還在草案階段，但，值得留意未來發展的動向：

1. ANAME

由於目前 CNAME 使用上會有所限制，例如：域名本身(example.tw)無法設定 CNAME 到別的域名，只能多指定一層 subdomain(www.example.tw)才能使用 CNAME 記錄。因此，當網站使用 CDN 服務時，域名本身卻只能設定 A 或 AAAA 記錄，而造成諸多不便。網站使用 CDN 的優勢，就是透過 CNAME 到 CDN 所提供的域名，讓 CDN 根據地區、服務等條件，自動對應到合適的 IP，以提供最佳的網站服務。因此，產生了新的

RR 類型(ANAME)的概念（目前是草案第 04 版），以解決 CNAME 無法設定域名本身的問題。

域名本身設定為 ANAME 時，當查詢該域名的 A 記錄時，Resolver 回傳的資料中，在 ANSWER 的區塊中，顯示該筆域名的 ANAME 及 A 記錄，並將 AAAA 記錄顯示在 ADDITIONAL 區塊中；反之，查詢 AAAA 記錄時，則將 A 記錄顯示在 ADDITIONAL 區塊中。若查詢該域名的 ANAME 記錄時，則將 A 與 AAAA 記錄顯示在 ADDITIONAL 中。



圖：DNSOP 工作小組討論現況

2. HTTPSSVC

新的 HTTPSSVC 類型（目前是草案第 03 版），則是希望當使用者要連線至 Web Server 時，可以先藉由事前的 DNS 查詢，將該網站的相關資料先行取得，以減少與網站在連線前階段的溝通次數，以加快與網站的連線速度。而且，HTTPSSVC 類型，也可以像 ANAME 類型一樣，將域名本身指定到另一個域名的相關記錄上。

每一筆 HTTPSSVC 記錄中，可以包含幾個主要資訊：

(1) ALIAS 域名：指定轉至那一筆 A 或 AAA 記錄。

(2) HTTP 版本:指定使用 HTTP/2 或 HTTP/3 的方式連線。
(3) PORT 編號:若不是使用預設的 443 port 時,可以指定 Web Server 使用的 port 編號。
(4) ESNIKEY 資料:將該網站使用的 ESNI 公鑰的資料放在 DNS 記錄中,讓使用者事先查詢 DNS 時,即可取得。

不過,因為該 RR 類型,將原本由 Web Server 的工作,提前至 DNS 主機,當網站流量增加時,是否也會造成 DNS 主機的過量負荷?則須持續關注該記錄類型的後續發展。

有關於域名註冊服務,使用 EPP(Extensible Provisioning Protocol)執行移轉註冊商時,為避免移轉未獲合法授權而被冒名盜取域名所有權,有一個新草案規範了此移轉流程,但,這因為涉及 ICANN 的政策決定,而不是技術問題,因此,最後是否會成為標準,必須持續觀察。此草案的重點敘述如下:

1. 原註冊商(registrar)僅在用戶提出移轉(transfer)申請時,才產生(設定)授權碼(authinfo code)並提供給用戶,這個授權碼是有有時效性,待時間到期,註冊商須將授權碼移除。
2. 註冊商不儲存授權碼資料,他是存放在註冊局(registry)。
3. 註冊局是儲存授權碼經過 HASH 後的資料,而非明碼儲存。因此,註冊商無法查詢原來的授權碼資料,只能以重新設定的方式更新授權碼資料。
4. 待域名成功移轉至新註冊商時,註冊局必須將授權碼資料移除。

IPv6 相關技術討論

本次參與有關 IPv6 技術討論會議,包括下列幾個工作小組:
1. v6ops Working Group - IPv6 Operations
2. 6MAN Working Group - IPv6 Maintenance,
3. 6lo Working Group - IPv6 over Networks of Resource-constrained Nodes,

各工作小組的介紹如下:
1. v6ops Working Group - IPv6 Operations

IPv6 運營工作組（v6ops）為新的和現有的 IPv6 網路的佈署和操作制定了指南。v6ops 工作組的目標是：

(1).徵求網路營運商和用戶的意見，以確定 IPv6 網路營運的問題，並確定這些問題的解決方案或解決方法。

(2).徵求網路營運商和用戶的意見，以確定與 IPv4 網路的營運交互問題，並確定這些問題的解決方案或解決方法。

(3).徵求對僅 IPv6 操作中的問題和機會的討論和記錄，以及由此產生的創新。

(4).已確定問題的營運解決方案應在 v6ops 中制訂，並記錄在訊息或 BCP 草案中。

(5).記錄 IPv6 網路的操作要求。

詳細 v6ops 工作組章程請參考：
https://datatracker.ietf.org/group/v6ops/about/

2. 6MAN Working Group - IPv6 Maintenance

6man 工作組負責維護和推進 IPv6 協議規範和尋址架構。工作組將解決在佈署和運行期間發現的協議限制/問題。6man 是 IPv6 協議擴展和修改的設計權威。

詳細 6MAN 工作組章程請參考：
https://datatracker.ietf.org/group/6man/about/

3. 6lo Working Group - IPv6 over Networks of Resource-constrained Nodes

6lo 專注於通過約束節點網路促進 IPv6 連接的工作，具有以下特點：

*有限的功率，內存和處理資源；

*狀態，代碼空間和處理週期的硬上限；

*能源和網路頻寬使用的優化；

*缺少一些第 2 層服務，如完整的設備連接和廣播/多播。

6lo 適用於小型，重點突出的工作，但不承擔更大的跨層工作。只要合理和可能，工作組將繼續重用現有的協議和機制。

詳細 6lo 工作組章程請參考：
https://datatracker.ietf.org/group/6lo/about/

會中進行的主題包含以下內容：

1. 464XLAT Optimization

本文為第三版發表於 IPv6 維運（IPv6 Operations，v6ops）工作小組，提出了可能的解決方案，以避免當目的地可用於 IPv6 時，IP / ICMP 轉換算法（SIIT）的某些缺點。 當 SIIT 用作 NAT46 且僅 IPv4 設備或應用程序啟動到雙協定 CDN（內容交付網絡），高速緩存或其他網路資源（在營運商網路或 Internet 中）的流量時，這些流量將轉通過 NAT64 換回 IPv4。這是 464XLAT 和 MAP-T 的情況。

詳細草案請參考：draft-palet-v6ops-464xlat-opt-cdn-caches-03

2. Neighbor Cache Entries on First-Hop Routers: Operational Considerations

本文為第一版發表於 IPv6 維運（IPv6 Operations，v6ops）工作小組，草案摘要如下：

Neighbor Discovery (RFC4861) is used by IPv6 nodes to determine the link-layer addresses of neighboring nodes as well as to discover and maintain reachability information. This document discusses how the neighbor discovery state machine on a first-hop router is causing user-visible connectivity issues when a new (not being seen on the network before) IPv6 address is being used.

詳細草案請參考：draft-linkova-v6ops-nd-cache-init-01

3. Operational Security Considerations for IPv6 Networks

本文為第 17 版發表於 IPv6 維運（IPv6 Operations，v6ops）工作小組，草案摘要如下：

Knowledge and experience on how to operate IPv4 securely is available: whether it is the Internet or an enterprise internal network. However, IPv6 presents some new security challenges. RFC 4942 describes the security issues in the protocol but network managers also need a more practical, operations-minded document to enumerate advantages and/or disadvantages of certain choices.

This document analyzes the operational security issues in several places of a network (enterprises, service providers and residential users) and proposes technical and procedural mitigations techniques. Some very specific places of a network such as the Internet of Things are not discussed in this document.

詳細草案請參考：draft-ietf-opsec-v6-17

4. IS-IS Multi Topology Deployment Considerations

本文為第 2 版發表於 IPv6 維運（IPv6 Operations，v6ops）工作小組，草案摘要如下：

This document analyzes IS-IS Multi Topology (MT) applicability in various deployments (Core/Mobile Backhaul/Data Center underlays). This document explores the nuances around the terminology and usage of various IS-IS address families, topologies with different considerations, for choosing the right combination for a specific deployment scenario.

This document also discusses various ways one can deploy IPv6 only IS-IS topology.

詳細草案請參考：draft-chunduri-lsr-isis-mt-deployment-cons-02

5. IPv6 Point-to-Point Links

本文為第 3 版發表於 IPv6 維運（IPv6 Operations，v6ops）工作小組，草案摘要如下：

This document describes different alternatives for configuring IPv6 point-to-point links, considering the prefix size, numbering choices and prefix pool to be used.

詳細草案請參考：draft-palet-v6ops-p2p-links-03

6. IPv6-Only Terminology Definition

本文為第 4 版發表於 IPv6 維運（IPv6 Operations，v6ops）工作小組，草案摘要如下：

This document defines the terminology regarding the usage of expressions such as "IPv6-only", in order to avoid confusions when using them in IETF and other documents. The goal is that the reference to "IPv6-only" describes the actual native

functionality being used, not the actual protocol support.

詳細草案請參考：draft-palet-v6ops-ipv6-only-04

7. IPv6 Segment Routing Header (SRH)

本文為第 21 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

Segment Routing can be applied to the IPv6 data plane using a new type of Routing Extension Header. This document describes the Segment Routing Extension Header and how it is used by Segment Routing capable nodes.

詳細草案請參考：draft-ietf-6man-segment-routing-header-21

8. ICMPv6 errors for discarding packets due to processing limits

本文為第 3 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

Network nodes may discard packets if they are unable to process protocol headers of packets due to processing constraints or limits. When such packets are dropped, the sender receives no indication so it cannot take action to address the cause of discarded packets. This document defines ICMPv6 errors that can be sent by a node that discards packets because it is unable to process the protocol headers. A node that receives such an ICMPv6 error may be able to modify what it sends in future packets to avoid subsequent packet discards.

詳細草案請參考：draft-ietf-6man-icmp-limits-03

9. IPv6 Minimum Path MTU Hop-by-Hop Option

本文為第 2 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

This document specifies a new Hop-by-Hop IPv6 option that is used to record the minimum Path MTU along the forward path between a source to a destination host. This collects a minimum recorded MTU along the path to the destination. The value can then be communicated back to the source using the return Path

MTU field in the option.

This Hop-by-Hop option is intended to be used in environments like Data Centers and on paths between Data Centers, to allow them to better take advantage of paths able to support a large Path MTU.

詳細草案請參考：draft-hinden-6man-mtu-option-02

10. IPv6 Neighbor Discovery on Wireless Networks

本文為第 3 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

This document describes how the original IPv6 Neighbor Discovery and Wireless ND (WiND) can be applied on various abstractions of wireless media.

詳細草案請參考：draft-thubert-6man-ipv6-over-wireless-03

11. IPv6 Neighbor Discovery Unicast Lookup

本文為第 1 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

This document updates RFC 8505 in order to enable unicast address lookup from a 6LoWPAN Border Router acting as an Address Registrar.

詳細草案請參考：draft-thubert-6lo-unicast-lookup-00

12. Discovering PREF64 in Router Advertisements

本文為第 3 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

This document specifies a Router Advertisement option to communicate NAT64 prefixes to clients.

詳細草案請參考：draft-ietf-6man-ra-pref64-03

13. IPv6 Support for Segment Routing: SRv6+

本文為第 4 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）

工作小組，草案摘要如下：

This document describes SRv6+. SRv6+ is a Segment Routing (SR) solution that leverages IPv6. It supports a wide variety of use-cases while remaining in strict compliance with IPv6 specifications. SRv6+ is optimized for for ASIC-based forwarding devices that operate at high data rates.

詳細草案請參考：draft-bonica-spring-srv6-plus-04

14. The IPv6 Compressed Routing Header (CRH)

本文為第 5 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

This document defines a new IPv6 Routing header type, called the Compressed Routing Header (CRH). SRv6+ nodes use the CRH to steer packets from segment to segment along SRv6+ paths.

詳細草案請參考：draft-bonica-6man-comp-rtg-hdr-05

15. The Per-Path Service Instruction (PPSI) Option

本文為第 6 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

SRv6+ encodes Per-Path Service Instructions (PPSI) in a new IPv6 option, called the PPSI Option. This document describes the PPSI Option.

詳細草案請參考：draft-bonica-6man-vpn-dest-opt-06

16. The Per-Segment Service Instruction (PSSI) Option

本文為第 4 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

SRv6+ encodes Per-Segment Service Instructions (PSSI) in a new IPv6 option, called the PSSI Option. This document describes the PSSI Option.

詳細草案請參考：draft-bonica-6man-seg-end-opt-04

17. Operations, Administration, and Maintenance (OAM) in Segment Routing Networks with IPv6 Data plane (SRv6)

本文為第 3 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

This document defines building blocks for Operations, Administration, and Maintenance (OAM) in Segment Routing Networks with IPv6 Dataplane (SRv6). The document also describes some SRv6 OAM mechanisms.

詳細草案請參考：draft-ali-6man-spring-srv6-oam-03

18. Service-aware IPv6 Network

本文為第 1 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

A multitude of applications are carried over the network, which have varying needs for network bandwidth, latency, jitter, and packet loss, etc. Some applications such as online gaming and live video streaming have very demanding network requirements thereof require special treatments in the network. However, since the current network is lack of enough information of service requirements of such applications it is difficult to guarantee the SLA or it may take long time to provide such guarantee. This document proposes the solution to make use of IPv6 extensions header to convey the service requirement information along with the packet to the network to facilitate the service deployment and network resource adjustment to guarantee SLA for applications. Then it defines the service-aware options which can be used in the different IPv6 extension headers for the purpose.

詳細草案請參考：draft-li-6man-service-aware-ipv6-network-00

19. Consideration of IPv6 Encapsulation for SFC and IFIT

本文為第 1 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

Service Function Chaining (SFC) and In-situ Flow Information Telemetry (IFIT) are important path services along with the packets. In order to support these services, several

encapsulations have been defined. The document analyzes the problems of these encapsulations in the IPv6 scenario and proposes the possible optimized encapsulation for IPv6.

詳細草案請參考：draft-li-6man-ipv6-sfc-ifit-01

20. Encapsulation of Path Segment in SRv6

本文為第 1 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

Segment Routing (SR) allows for a flexible definition of end-to-end paths by encoding paths as sequences of sub-paths, called "segments". Segment routing architecture can be implemented over IPv6 data plane, called SRv6. In some use-cases such as end-to-end SR Path Protection and Performance Measurement (PM), SRv6 path need to be identified. This document defines the encoding and processing of Path Segment in SRv6 networks.

詳細草案請參考：draft-li-6man-srv6-path-segment-encap-00

21. Segment Routing Header encapsulation for In-situ OAM Data

本文為第 1 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

OAM and PM information from the SR endpoints can be piggybacked in the data packet. The OAM and PM information piggybacking in the data packets is also known as In-situ OAM (IOAM). IOAM records operational and telemetry information in the data packet while the packet traverses a path between two points in the network. This document defines how IOAM data fields are transported as part of the Segment Routing with IPv6 data plane (SRv6) header.

詳細草案請參考：draft-ali-spring-ioam-srv6-01

22. DetNet SRv6 Data Plane Encapsulation

本文為第 1 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

This document specifies Deterministic Networking data plane operation for SRv6 encapsulated user data.

詳細草案請參考：draft-geng-detnet-dp-sol-srv6-01

23. Transmission of IPv6 Packets over Near Field Communication

本文為第 15 版發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，草案摘要如下：

Near field communication (NFC) is a set of standards for smartphones and portable devices to establish radio communication with each other by touching them together or bringing them into proximity, usually no more than 10 cm apart. NFC standards cover communications protocols and data exchange formats, and are based on existing radio-frequency identification (RFID) standards including ISO/IEC 14443 and FeliCa. The standards include ISO/IEC 18092 and those defined by the NFC Forum. The NFC technology has been widely implemented and available in mobile phones, laptop computers, and many other devices. This document describes how IPv6 is transmitted over NFC using 6LoWPAN techniques.

詳細草案請參考：draft-ietf-6lo-nfc-15

24. Packet Delivery Deadline time in 6LoWPAN Routing Header

本文為第 5 版發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，草案摘要如下：

This document specifies a new type for the 6LoWPAN routing header containing the deadline time for data packets, designed for use over constrained networks. The deadline time enables forwarding and scheduling decisions for time critical IoT machine to machine (M2M) applications that operate within time-synchronized networks that agree on the meaning of the time representations used for the deadline time values.

詳細草案請參考：draft-ietf-6lo-deadline-time-05

25. 6LoWPAN Fragment Forwarding

本文為第 3 版發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，草案摘要如下：

This document provides a simple method to forwarding 6LoWPAN fragments. When employing adaptation layer fragmentation in 6LoWPAN, it may be beneficial for a forwarder not to have to reassemble each packet in its entirety before forwarding it. This has always been possible with the original fragmentation design of RFC4944. This method reduces the latency and increases end-to-end reliability in route-over forwarding. It is the companion to the virtual Reassembly Buffer which is a pure implementation technique.

詳細草案請參考：draft-ietf-6lo-minimal-fragment-03

26. 6LoWPAN Selective Fragment Recovery

本文為第 5 版發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，草案摘要如下：

This draft updates RFC 4944 with a simple protocol to recover individual fragments across a route-over mesh network, with a minimal flow control to protect the network against bloat.

詳細草案請參考：draft-ietf-6lo-fragment-recovery-05

27. IPv6 over Constrained Node Networks (6lo) Applicability & Use cases

本文為第 6 版發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，草案摘要如下：

This document describes the applicability of IPv6 over constrained node networks (6lo) and provides practical deployment examples. In addition to IEEE 802.15.4, various link layer technologies such as ITU-T G.9959 (Z-Wave), BLE, DECT-ULE, MS/TP, NFC, PLC (IEEE 1901.2), and IEEE 802.15.4e (6tisch) are used as examples. The document targets

an audience who like to understand and evaluate running end-to-end IPv6 over the constrained node networks connecting devices to each other or to other devices on the Internet (e.g. cloud infrastructure).

詳細草案請參考：draft-ietf-6lo-use-cases-06

28. IPv6 Neighbor Discovery Unicast Lookup

本文為第 1 版發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，草案摘要如下：

This document updates RFC 8505 in order to enable unicast address lookup from a 6LoWPAN Border Router acting as an Address Registrar.

詳細草案請參考：draft-thubert-6lo-unicast-lookup-00

29. Asymmetric IPv6 for IoT Networks

本文為第 1 版發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，草案摘要如下：

This document describes a new approach to IPv6 header compression for use in scenarios where minimizing packet size is crucial but routing performance must be maximised.

詳細草案請參考：draft-jiang-asymmetric-ipv6-01

IoT 相關技術討論

本次參與有關 IoT 技術討論會議，包括下列幾個工作小組：

1. suit Working Group - Software Updates for Internet of Things；
2. 6TiSCH Working Group - IPv6 over the TSCH mode of IEEE 802.15.4e；(TSCH is the abbreviation of Time Slotted Channel Hopping)
3. lpwan Working Group - IPv6 over Low Power Wide-Area Networks；
4. t2trg Working Group - Thing-to-Thing。

各工作小組的介紹如下：

1. suit Working Group - Software Updates for Internet of Things；

物聯網（IoT）設備中的漏洞引發了對安全韌體更新機制的需求，該機制也適用於受約束設備。安全專家，研究人員和監管機構建議所有物聯網設備都配備這樣的機制。

韌體更新解決方案包含多個組件，包括：

*將韌體映像傳輸到相容設備的機制。

*提供有關韌體映像的後設資料(meta-data)清單（例如韌體包標識符，程序包需要運行的硬體以及對其他韌體包的依賴性），以及用於保護韌體映像的加密信息。

*韌體映像本身。

詳細 suit 工作組章程請參考：
https://datatracker.ietf.org/group/suit/about/

2. 6TiSCH Working Group - IPv6 over the TSCH mode of IEEE 802.15.4e；(TSCH is the abbreviation of Time Slotted Channel Hopping)

低功耗和有損網路（Low-power and Lossy Networks，LLN）將可能因大量的資源受限節點互連以形成無線網狀網路。IEEE802.15.4TSCH 網路中的節點通過遵循時分多址（TDMA）調度進行通訊。該調度中的時隙提供了為相鄰節點之間的通訊分配的頻寬單位。可以對分配進行編程，使得可預測的傳輸模式與流量匹配。

這些技術為 LLN 提供了一系列新的使用案例，包括：

- 無線過程控制網路中的控制環路，其中需要高可靠性和完全確定性的行為。
- 從不同的獨立客戶端傳輸數據的服務提供商網路，營運商需要流量隔離和流量整形。
- 包括能量收集節點的網路，其需要極低且可預測的平均功耗。

詳細 6TiSCH 工作組章程請參考：
https://datatracker.ietf.org/group/6tisch/about/

3. lpwan Working Group - IPv6 over Low Power Wide-Area Networks；

新一代無線技術以低功耗廣域（LPWA）的通用名稱出現，具有許多共同特徵，使這些技術成為物聯網應用的獨特和破壞性。

為了釋放 LPWA 技術及其生態系統的全部功能，需要將它們與其他生態系統相結合，通過引入網路層來保證交互工作，並為管理和安全性以及共享應用程序配置文件啟用通用組件。IETF 可以通過提供 IPv6 連接做出貢獻，並提出保護操作和管理設備及其網關的技術。

工作組將重點關注通過以下選擇的低功耗廣域技術實現 IPv6 連接：SIGFOX，LoRa，WI-SUN 和 NB-IOT。

詳細 lpwan 工作組章程請參考：
https://datatracker.ietf.org/group/lpwan/about/

4. t2trg Working Group - Thing-to-Thing。

該物對物的研究組（T2TRG）將開放研究一個真正的“物聯網”變為現實的問題。物聯網其中低資源節點能夠之間溝通自己和與更廣泛的互聯網，以參與無權創新。T2TRG 的重點將從設備連接到 IP 的適配層開始，並在應用層結束。具有用於通訊和製作數據和管理功能的架構和 API（包括安全功能）。

工作組已經確定了一些感興趣的領域，包括：
*了解單用途筒倉和網關的動機，促進小塊鬆散地連接（因此“物到物”）；支持擴展單個網路中的應用程序數量。
*部署注意事項； 規模考量； 擁有成本。
*“物”的管理和操作。
*生命週期方面（包括但不限於安全性考慮）。
*與 W3C 的合作，例如，數據模型，格式和語義。

詳細 t2trg 工作組章程請參考：
https://datatracker.ietf.org/group/t2trg/about/

會中進行的主題包含以下內容：

1. A Firmware Update Architecture for Internet of Things Devices

本文為第 5 版發表於物聯網軟體更新（Software Updates for Internet of Things，suit）工作小組，草案摘要如下：

Vulnerabilities with Internet of Things (IoT) devices have raised the need for a solid and secure firmware update mechanism that is also suitable for constrained devices. Incorporating such update mechanism to fix vulnerabilities, to update configuration settings as well as adding new functionality is recommended by security experts.

This document lists requirements and describes an architecture for a firmware update mechanism suitable for IoT devices. The architecture is agnostic to the transport of the firmware images and associated meta-data.

This version of the document assumes asymmetric cryptography and a public key infrastructure. Future versions may also describe a symmetric key approach for very constrained devices.

詳細草案請參考：draft-ietf-suit-architecture-05

2. Firmware Updates for Internet of Things Devices - An Information Model for Manifests

本文為第 3 版發表於物聯網軟體更新（Software Updates for Internet of Things，suit）工作小組，草案摘要如下：

Vulnerabilities with Internet of Things (IoT) devices have raised the need for a solid and secure firmware update mechanism that is also suitable for constrained devices. Incorporating such an update mechanism to fix vulnerabilities, to update configuration settings, as well as adding new functionality is recommended by security experts.

One component of such a firmware update is a concise and machine-processable meta-data document, or manifest, that describes the firmware image(s) and offers appropriate protection. This document describes the information that must be present in the manifest.

詳細草案請參考：draft-ietf-suit-information-model-03

3. SUIT CBOR manifest serialisation format

本文為第 5 版發表於物聯網軟體更新（Software Updates for Internet of Things，suit）工作小組，草案摘要如下：

This specification describes the format of a manifest. A manifest is a bundle of metadata about the firmware for an IoT device, where to find the firmware, the devices to which it applies, and cryptographic information protecting the manifest.

詳細草案請參考：draft-moran-suit-manifest-05

4. An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4

本文為第 24 版發表於 IPv6 基於 IEEE 802.15.4e 的 TSCH 模式（IPv6 over the TSCH mode of IEEE 802.15.4e，6TiSCH）工作小組，草案摘要如下：

This document describes a network architecture that provides low-latency, low-jitter and high-reliability packet delivery. It combines a high-speed powered backbone and subnetworks using IEEE 802.15.4 time-slotted channel hopping (TSCH) to meet the requirements of LowPower wireless deterministic applications.

詳細草案請參考：
draft-ietf-6tisch-architecture-24

5. Minimal Security Framework for 6TiSCH

本文為第 12 版發表於 IPv6 基於 IEEE 802.15.4e 的 TSCH 模式（IPv6 over the TSCH mode of IEEE 802.15.4e，6TiSCH）工作小組，草案摘要如下：

This document describes the minimal framework required for a new device, called "pledge", to securely join a 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4e) network. The framework requires that the pledge and the JRC (join registrar/coordinator, a central entity), share a symmetric key. How this key is provisioned is out of scope of this document. Through a single CoAP (Constrained Application Protocol) request-response exchange secured by OSCORE (Object Security for Constrained RESTful Environments), the pledge requests admission into the network and the JRC configures it with

link-layer keying material and other parameters. The JRC may at any time update the parameters through another request-response exchange secured by OSCORE. This specification defines the Constrained Join Protocol and its CBOR (Concise Binary Object Representation) data structures, and configures the rest of the 6TiSCH communication stack for this join process to occur in a secure manner. Additional security mechanisms may be added on top of this minimal framework.

詳細草案請參考：draft-ietf-6tisch-minimal-security-12

6. 6tisch Zero-Touch Secure Join protocol

本文為第 4 版發表於 IPv6 基於 IEEE 802.15.4e 的 TSCH 模式（IPv6 over the TSCH mode of IEEE 802.15.4e，6TiSCH）工作小組，草案摘要如下：

This document describes a Zero-touch Secure Join (ZSJ) mechanism to enroll a new device (the "pledge") into a IEEE802.15.4 TSCH network using the 6tisch signaling mechanisms. The resulting device will obtain a domain specific credential that can be used with either 802.15.9 per-host pair keying protocols, or to obtain the network-wide key from a coordinator.

The mechanism describe here is an augmentation to the one-touch mechanism described in [I-D.ietf-6tisch-minimal-security], and is a profile of the constrained voucher mechanism [I-D.ietf-anima-constrained-voucher].

詳細草案請參考：draft-ietf-6tisch-dtsecurity-zerotouch-join-04

7. IEEE802.15.4 Informational Element encapsulation of 6tisch Join and Enrollment Information

本文為第 1 版發表於 IPv6 基於 IEEE 802.15.4e 的 TSCH 模式（IPv6 over the TSCH mode of IEEE 802.15.4e，6TiSCH）工作小組，草案摘要如下：

In TSCH mode of IEEE802.15.4, as described by [RFC8180], opportunities for broadcasts are limited to specific times and specific channels. Nodes in a TSCH network typically frequently send Enhanced Beacon (EB) frames to announce the presence of the network. This document provides a mechanism by which small

details critical for new nodes (pledges) and long sleeping nodes may be carried within the Enhanced Beacon.

詳細草案請參考：
draft-ietf-6tisch-enrollment-enhanced-beacon-01

8. 6TiSCH Minimal Scheduling Function (MSF)

本文為第 5 版發表於 IPv6 基於 IEEE 802.15.4e 的 TSCH 模式（IPv6 over the TSCH mode of IEEE 802.15.4e，6TiSCH）工作小組，草案摘要如下：

This specification defines the 6TiSCH Minimal Scheduling Function (MSF). This Scheduling Function describes both the behavior of a node when joining the network, and how the communication schedule is managed in a distributed fashion. MSF builds upon the 6TiSCH Operation Sublayer Protocol (6P) and the Minimal Security Framework for 6TiSCH.

詳細草案請參考：draft-ietf-6tisch-msf-05

9. Robust Scheduling against Selective Jamming in 6TiSCH Networks

本文為第 2 版發表於 IPv6 基於 IEEE 802.15.4e 的 TSCH 模式（IPv6 over the TSCH mode of IEEE 802.15.4e，6TiSCH）工作小組，草案摘要如下：

This document defines a method to generate robust TSCH schedules in a 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4-2015) network, so as to protect network nodes against selective jamming attack. Network nodes independently compute the new schedule at each slotframe, by altering the one originally available from 6top or alternative protocols, while preserving a consistent and collision-free communication pattern. This method can be added on top of the minimal security framework for 6TiSCH.

詳細草案請參考：draft-tiloca-6tisch-robust-scheduling-02

10. LPWAN Static Context Header Compression (SCHC) and fragmentation for IPv6 and UDP

本文為第 18 版發表於 IPv6 低功耗廣域網路(IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

This document defines the Static Context Header Compression (SCHC) framework, which provides both header compression and fragmentation functionalities. SCHC has been designed for Low Power Wide Area Networks (LPWAN).

SCHC compression is based on a common static context stored in both the LPWAN device and the network side. This document defines a header compression mechanism and its application to compress IPv6/UDP headers.

This document also specifies a fragmentation and reassembly mechanism that is used to support the IPv6 MTU requirement over the LPWAN technologies. Fragmentation is needed for IPv6 datagrams that, after SCHC compression or when such compression was not possible, still exceed the layer-2 maximum payload size.

The SCHC header compression and fragmentation mechanisms are independent of the specific LPWAN technology over which they are used. This document defines generic functionalities and offers flexibility with regard to parameter settings and mechanism choices.

This document standardizes the exchange over the LPWAN between two SCHC entities. Settings and choices specific to a technology or a product are expected to be grouped into profiles, which are specified in other documents. Data models for the context and profiles are out of scope.

詳細草案請參考：draft-ietf-lpwan-ipv6-static-context-hc-18

11.SCHC over Sigfox LPWAN

本文為第 1 版發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

The Static Context Header Compression (SCHC) specification describes a header compression scheme and a fragmentation functionality for Low Power Wide Area Network (LPWAN) technologies. SCHC offers a great level of flexibility that can be tailored for different LPWAN technologies.

The present document provides the optimal parameters and modes of operation when SCHC is implemented over a Sigfox LPWAN.

詳細草案請參考：draft-ietf-lpwan-schc-over-sigfox-00

12.Static Context Header Compression (SCHC) over LoRaWAN

本文為第 2 版發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

The Static Context Header Compression (SCHC) specification describes generic header compression and fragmentation techniques for LPWAN (Low Power Wide Area Networks) technologies. SCHC is a generic mechanism designed for great flexibility, so that it can be adapted for any of the LPWAN technologies.

This document provides the adaptation of SCHC for use in LoRaWAN networks, and provides elements such as efficient parameterization and modes of operation. This is called a profile.

詳細草案請參考：draft-ietf-lpwan-schc-over-lorawan-02

13.Data Model for Static Context Header Compression (SCHC)

本文為第 1 版發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

This document describes a YANG data model for the SCHC (Static Context Header Compression). A generic module is defined, that can be applied for any headers and also a specific model for the IPv6 UDP protocol stack is also proposed. Note that this draft is a first attempt to define a YANG data module for SCHC, more work is needed to use all the YANG facilities.

詳細草案請參考：draft-toutain-lpwan-schc-yang-data-model-00

14.LPWAN Static Context Header Compression (SCHC) for CoAP

本文為第 9 版發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

This draft defines the way SCHC header compression can be applied to CoAP headers. CoAP header structure differs from IPv6 and UDP protocols since the CoAP use a flexible header with a variable number of options themself of a variable length.

Another important difference is the asymmetry in the header format used in request and response messages. Most of the compression mechanisms have been introduced in [I-D.ietf-lpwan-ipv6-static-context-hc], this document explains how to use the SCHC compression for CoAP.

詳細草案請參考：draft-ietf-lpwan-coap-static-context-hc-09

15.OAM for LPWAN using Static Context Header Compression (SCHC)

本文為第 1 版發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

With IP protocols now generalizing to constrained networks, users expect to be able to Operate, Administer and Maintain them with the familiar tools and protocols they already use on less constrained networks.

OAM uses specific messages sent into the data plane to measure some parameters of a network. Most of the time, no explicit values are sent is these messages. Network parameters are obtained from the analysis of these specific messages.

This can be used:

- To detect if a host is up or down.
- To measure the RTT and its variation over time.
- To learn the path used by packets to reach a destination.

-AM in LPWAN is a little bit trickier since the bandwidth is limited and extra traffic added by OAM can introduce perturbation on regular transmission.

Two scenarios can be investigated:

- OAM coming from internet. In that case, the NGW should act as a proxy and handle specifically the OAM traffic.
- OAM coming from LPWAN devices: This can be included into regular devices but some specific devices may be installed in the LPWAN network to measure its quality.

The primitive functionalities of OAM are achieved with the ICMPv6 protocol.

ICMPv6 defines messages that inform the source of IPv6 packets of errors during packet delivery. It also defines the Echo Request/Reply messages that are used for basic network troubleshooting (ping command). ICMPv6 messages are transported on IPv6.

This document describes how basic OAM is performed on Low Power Wide Area Networks (LPWANs) by compressing ICMPv6/IPv6 headers and by protecting the LPWAN network and the Device from undesirable ICMPv6 traffic.

詳細草案請參考：draft-barthel-lpwan-oam-schc-00

16.RTO considerations in LPWAN

本文為第 1 版發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

Low-Power Wide Area Network (LPWAN) technologies are characterized by very low physical layer bit and message transmission rates. Moreover, a response to a message sent by an LPWAN device may often only be received after a significant delay. As a result, Round-Trip Time (RTT) values in LPWAN are often (sometimes, significantly) greater than typical default values of Retransmission TimeOut (RTO) algorithms. Furthermore, buffering at network elements such as radio gateways may interact negatively with LPWAN technology transmission mechanisms, potentially exacerbating RTTs by up to several orders of magnitude. This document provides guidance for RTO settings in LPWAN, and describes an experimental dual RTO algorithm for LPWAN.

詳細草案請參考：draft-gomez-rto-considerations-lpwan-00

17.RESTful Design for Internet of Things Systems

本文為第 4 版發表於物到物（Thing-to-Thing，t2trg）工作小組，草案摘要如下：

This document gives guidance for designing Internet of Things (IoT) systems that follow the principles of the Representational State Transfer (REST) architectural style. This document is a product of the IRTF Thing-to-Thing Research Group (T2TRG).

詳細草案請參考：draft-irtf-t2trg-rest-iot-04

18.YANG Object Universal Parsing Interface

本文為第 1 版發表於物到物（Thing-to-Thing，t2trg）工作

小組，草案摘要如下：

YANG Object Universal Parsing Interface (YOUPI) specification describes generic way to encode and decode binary data based on a YANG model for use of constrainted devices. YOUPI is a generic mechanism designed for great flexibility, so that it can be adapted for any of the constainted devices.

詳細草案請參考：draft-petrov-t2trg-youpi-00

19.Problem Statement of IoT integrated with Edge Computing

本文為第 1 版發表於物到物（Thing-to-Thing，t2trg）工作小組，草案摘要如下：

This document describes new challenges such as strict latency, uplink cost, uninterrupted services, privacy and security, for IoT services originated from the IoT environmental changes. In order to address those new challenges, the integration of Edge computing and IoT has been emerged as a promising solution. This document discribes the concept of IoT integrated with Edge computing as well as the state-of-the-art of IoT Edge computing. It also proposes an architecture of IoT Edge computing. The direction of Edge computing for IoT should be discussed in the IETF/IRTF.

詳細草案請參考：draft-hong-t2trg-iot-edge-computing-00

路由安全維運相關技術討論

本次參與有關路由安全維運技術的討論會議，sidrops 工作小組，sidrops Working Group - SIDR Operations 工作小組的介紹如下：

SIDR 的全球部署，正在進行包括 RPKI，BGP 來源公告驗證和 BGPSEC，以創建一個由 SIDR 感知和非 SIDR 感知網路組成的網際網路路由系統。

此部署必須正確處理，以避免將 Internet 劃分為單獨的網路。Sidrops 負責鼓勵部署 SIDR 技術，同時確保在過渡期間盡可能保證全球路由系統的安全。

SIDR 營運工作組（sidrops）為 SIDR 感知網路的營運制定指南，並提供有關如何在現有網路和新網路中部署和運行 SIDR 技術。

sidrops 工作組專注於 SIDR 技術的部署和營運問題及經驗，這些技術包括全球路由系統，以及構成 SIDR 架構的存儲庫和 CA 系統。

詳細 sidrops 工作組章程請參考：
https://datatracker.ietf.org/group/sidrops/about/

SIDR 營運工作組（sidrops）於會中進行的主題包含以下內容：

1. A Profile for Autonomous System Provider Authorization

   本文為第 1 版發表於 SIDR 營運（SIDR Operations，sidrops）工作小組，草案摘要如下：

   This document defines a standard profile for Autonomous System Provider Authorization in the Resource Public Key Infrastructure. An Autonomous System Provider Authorization is a digitally signed object that provides a means of verifying that a Customer Autonomous System holder has authorized a Provider Autonomous System to be its upstream provider and for the Provider to send prefixes received from the Customer Autonomous System in all directions including providers and peers.

   詳細草案請參考：draft-ietf-sidrops-aspa-profile-00

2. Verification of AS_PATH Using the Resource Certificate Public Key Infrastructure and Autonomous System Provider Authorization

   本文為第 1 版發表於 SIDR 營運（SIDR Operations，sidrops）工作小組，草案摘要如下：

   This document defines the semantics of an Autonomous System Provider Authorization object in the Resource Public Key Infrastructure to verify the AS_PATH attribute of routes advertised in the Border Gateway Protocol.

   詳細草案請參考：draft-ietf-sidrops-aspa-verification-01

3. Signaling Prefix Origin Validation Results from an RPKI Origin Validating BGP Speaker to BGP Peers

   本文為第 3 版發表於 SIDR 營運（SIDR Operations，sidrops）工作小組，草案摘要如下：

   This document describes the use of BGP large communities,

as well as its usage, to signal prefix origin validation results from an RPKI Origin validating BGP speaker to other BGP peers. Upon reception of prefix origin validation results, peers can use this information in their local routing decision process.

詳細草案請參考：draft-ietf-sidrops-validating-bgp-speaker-03

4. RPKI Signed Object for Trust Anchor Keys

本文為第3版發表於SIDR營運（SIDR Operations，sidrops）工作小組，草案摘要如下：

Trust Anchor Locators (TALs) [I-D.ietf-sidrops-https-tal] are used by Relying Parties in the RPKI to locate and validate Trust Anchor certificates used in RPKI validation. This document defines an RPKI signed object for Trust Anchor Keys (TAK), that can be used by Trust Anchors to signal their set of current keys and the location(s) of the accompanying CA certiifcates to Relying Parties, as well as changes to this set in the form of revoked keys and new keys, in order to support both planned and unplanned key rolls without impacting RPKI validation.

詳細草案請參考：draft-ietf-sidrops-signed-tal-03

四、 建議意見：

建議事項

☐ 建議持續關注相關各 WGs 動態及相關訊息。
☐ IPv6 技術規範已有 IPv6-only 以及因應物聯網需求的草案提出，建議持續關注IPv6的相關技術規範發展，強化新一代網路基礎建設。
☐ 物聯網相關技術規範，廣泛地從架構，軟體，安全，應用，格式等各方面都有草案提出，建議持續關注 IoT 的相關技術規範發展，以取得新一代網路應用技術，作為創新產業的基礎。
☐ 建議持續關注 DNS 的相關技術發展，以掌握最新的發展趨勢。
☐ 建議持續了解 EPP 的政策規範，以配合修改相關作業流程。
☐ 建議與國外相關單位進行更密切及多元的交流及經驗分享。
☐ 建議持續參與 IETF 以掌握相關技術規範的演進及狀態。

IETF 下一次會議將於 2019 年 11 月 16-22 日於新加坡舉行，相關資訊請參考 https://www.ietf.org/how/meetings/106/。

五、 會議議程：

以下為 IETF 104 Prague 的完整議程表：

Saturday, July 20, 2019 (EDT)	
時間	議程
8:30-22:00	IETF Hackathon
9:30-18:00	Code Sprint

Sunday, July 21, 2019 (EDT)	
時間	議程
8:30-16:00	IETF Hackathon
10:00-12:00	IEPG Meeting
10:00-18:00	IETF Registration
12:30-13:30	Tutorial: Newcomers' Overview
13:45-14:45	Tutorial: Writing Security Considerations
16:00-17:00	Newcomers' Quick Connections (Open to Newcomers. Note that pre-registration is required)
17:00-19:00	Welcome Reception
18:00-20:00	Sunday Hot RFC lightning talks

Monday, July 22, 2019 (EDT)	
時間	議程
8:00-9:00	Continental Breakfast
8:00-9:00	Systers Networking Event
8:30-9:45	Side Meetings / Open Time
8:30-18:30	IETF Registration
9:00-19:10	IRTF Applied Networking Research Workshop (ANRW)
10:00-12:00	Internet Area AD Office Hours
10:00-12:00	**Monday Morning session I**
	Captive Portal Interaction 1000 – 1100
	Secure Telephone Identity Revisited 1100 - 1200
	Benchmarking Methodology
	Network Configuration
	Routing Area Working Group
	Automated Certificate Management Environment

	Trusted Execution Environment Provisioning
	Local Optimizations on Path Segments (BOF)
12:00-13:30	Break
12:15-13:15	SEC AD Office Hours
13:30-15:30	**Monday Afternoon session I**
	IPv6 over Networks of Resource-constrained Nodes
	Media OPerationS (BOF)
	Network Modeling
	Locator/ID Separation Protocol
	Link State Routing
	Security Dispatch
	Transport Services
15:30-15:50	Beverage and Snack Break
15:50-17:50	**Monday Afternoon session II**
	Hypertext Transfer Protocol
	Network Time Protocol
	Network Modeling
	IPv6 Operations
	Multiprotocol Label Switching
	Lightweight Authenticated Key Exchange (BOF)
	Multipath TCP
18:10-19:40	Hackdemo Happy Hour
18:10-19:10	**Monday Afternoon session III**
	Dispatch Joint with ARTAREA
	Domain Name System Operations
	Link State Routing
	Managed Incident Lightweight Exchange
19:30-21:00	Newcomers' Dinner

Tuesday, July 23, 2019 (EDT)	
時間	議程
8:00-9:00	Continental Breakfast
8:30-9:45	Side Meetings / Open Time
8:30-17:30	IETF Registration
8:30-9:45	**Tuesday Side meetings / open time**

	Technology Deep Dive : How NICs Work Today
10:00-12:00	**Tuesday Morning session I**
	Concise Binary Object Representation Maintenance and Extensions 1000-1130
	IP Wireless Access in Vehicular Environments 1130-1200
	Human Rights Protocol Considerations
	Information-Centric Networking
	Autonomic Networking Integrated Model and Approach
	Domain Name System Operations
	Routing Area Working Group
	Trusted Execution Environment Provisioning
	QUIC
12:00-13:30	Break
13:30-15:00	**Tuesday Afternoon session I**
	Applications Doing DNS (BOF)
	Global Access to the Internet for All
	Internet Congestion Control
	Autonomic Networking Integrated Model and Approach
	Traffic Engineering Architecture and Signaling
	Limited Additional Mechanisms for PKIX and SMIME
	Security Events
15:00-15:20	Beverage and Snack Break
15:20-16:50	**Tuesday Afternoon session II**
	Relay User Machine
	Internet Area Working Group
	IRTF Open Meeting
	SIDR Operations
	BGP Enabled ServiceS
	Traffic Engineering Architecture and Signaling
	IP Security Maintenance and Extensions
	Web Authorization Protocol
17:10-18:10	**Tuesday Afternoon session III**
	Audio/Video Transport Core Maintenance
	Constrained RESTful Environments
	IPv6 Maintenance
	Bidirectional Forwarding Detection

	Mobile Ad-hoc Networks
	Transport Layer Security
18:30-22:00	IETF 105 Social Event

Wednesday, July 24, 2019 (EDT)	
時間	議程
8:00-9:00	Continental Breakfast
8:30-9:45	Side Meetings / Open Time
8:30-17:10	IETF Registration
9:00-9:45	Routing AD Office Hours
10:00-12:00	**Wednesday Morning session I**
	Distributed Mobility Management
	Decentralized Internet Infrastructure
	Operations and Management Area Working Group
	Routing Over Low power and Lossy networks
	Source Packet Routing in Networking
	DDoS Open Threat Signaling
	Software Updates for Internet of Things
	QUIC
12:00-13:30	Break
12:15-13:15	WG Chairs Forum
13:30-15:30	**Wednesday Afternoon session I**
	IETF Meeting Network Requirements (BOF)
	Privacy Enhancements and Assessments Research Group
	Thing-to-Thing
	Bit Indexed Explicit Replication
	Deterministic Networking
	Inter-Domain Routing
	EAP Method Update
	IP Performance Measurement
15:30-15:50	Beverage Break
15:50-16:50	TSV AD Office Hours
15:50-16:50	**Wednesday Afternoon session II**
	Calendaring Extensions
	Global Routing Operations
	Babel routing protocol

	Deterministic Networking
	Remote ATtestation ProcedureS
16:50-17:10	Beverage and Snack Break
17:10-18:10	**IETF Technical Plenary**
18:20-19:50	**IETF Administrative/Operations Plenary**

Thursday, July 25, 2019 (EDT)	
時間	**議程**
8:00-9:00	Continental Breakfast
8:00-9:00	Newcomers' Feedback Session
8:30-9:45	Side Meetings / Open Time
8:30-18:00	IETF Registration
10:00-12:00	**Thursday Morning session I**
	Constrained RESTful Environments
	Registration Protocols Extensions
	Link State Vector Routing
	Path Computation Element
	Interface to Network Security Functions
	Transport Layer Security
	Application-Layer Traffic Optimization
	Transport Area Working Group
12:00-13:30	Break
12:15-13:15	Systers Lunch
13:30-15:30	**Thursday Afternoon session I**
	Extensions for Scalable DNS Service Discovery
	Computing in the Network Proposed Research Group
	Path Aware Networking RG
	Common Control and Measurement Plane
	Protocols for IP Multicast
	Security Area Open Meeting
	Network File System Version 4
	TCP Maintenance and Minor Extensions
15:30-15:50	Beverage and Snack Break
15:50-17:20	**Thursday Afternoon session II**
	Hypertext Transfer Protocol
	IPv6 Maintenance

	DNS PRIVate Exchange
	Crypto Forum
	MBONE Deployment
	Routing In Fat Trees
	Remote ATtestation ProcedureS
	Transport Area Open Meeting
17:20-17:40	Beverage Break
17:40-19:10	**Thursday Afternoon session III**
	IPv6 over the TSCH mode of IEEE 802.15.4e
	Network Management
	BGP Enabled ServiceS
	Authentication and Authorization for Constrained Environments
	Security Automation and Continuous Monitoring
	RTP Media Congestion Avoidance Techniques

Friday, July 26, 2019 (EDT)	
時間	**議程**
8:00-9:00	Continental Breakfast
8:30-9:45	Side Meetings / Open Time
8:30-12:20	IETF Registration
10:00-12:00	**Friday Morning session I**
	IPv6 over Low Power Wide-Area Networks
	Measurement and Analysis for Protocols
	Coding for efficient NetWork Communications Research Group
	Inter-Domain Routing
	Messaging Layer Security
	Web Authorization Protocol
	Delay/Disruption Tolerant Networking
12:00-12:20	Beverage and Snack Break
12:20-13:50	**Friday Afternoon session I**
	JSON Mail Access Protocol
	Inter-Domain Routing
	Network Virtualization Overlays
	CBOR Object Signing and Encryption
	Transport Area Working Group